The Future of Ransomware and Social Engineering

Understanding Ransomware Trends, Users, and the Malicious Social Engineering Tactics They Use

2017 Aug 24

Extortion is a tactic that has long been used by criminals for financial gain. Digital extortion through ransomware continues to represent a significant cyber threat to individuals, small businesses, corporations, and government entities. While cyber attacks are generally considered as technical exercises, successful ransomware operations employ social engineering tactics to help identify and exploit target vulnerabilities. Private sector, non-governmental organization (NGO), and government analysts were brought together by the Office of the Director of National Intelligence and the Department of Homeland Security to examine the current state of ransomware, understand how social engineering tactics are currently employed, and how ransomware attacks may change over the next two years. In this paper, ransomware is defined as malicious software that blocks access to computer systems or files until money is paid. Social engineering is defined as using human interaction to psychologically manipulate targets through deception and persuasion in order to influence the target's actions.

2017 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

The Future of Ransomware and Social Engineering
Team Members

Name	Organization
Peter M. (Champion)	FBI
Ross Albert	HUB International
Konstantin B.	FBI
Aric Jimenez	Southwest Texas Fusion Center
Shane Keane	Stratheron, LLC
Steve Mancini	NCFTA
Michael Orr	BP
Rob Pantazopoulos	Financial Industry
Patricia P.	FBI
Ashley Reichert	Illinois Statewide Terrorism and Intelligence Center
Kelly Wentzel	Wisconsin Statewide Intelligence Center

Key Judgments

- While ransomware will continue to be used by financially motivated cyber actors, it will likely be increasingly used for other purposes such as denial and deception, or combined with other cyber techniques.
- Cyber criminals may threaten to publish data online to extort additional ransom from the victim
- A ransomware attack can impact all facets of an organization. While the initial impact may be limited to whether the victim pays the ransom or not, the long-term effects of an attack may be far more extensive and costly
- The number of attacks will increase due to proliferation of ransomware tools
- Ransomware attacks will likely expand to include targeting of Internet of Things (IoT) devices
- Social engineering will remain one of the easiest ways for a cybercriminal to gain access to a computer system to deploy a ransomware attack. A variety of techniques that include technology and methods of human manipulation will continue to be employed to collect this information.

Scope

This paper was prepared by the Future of Ransomware and Social Engineering team, operating under the auspices of the Department of Homeland Security's Analyst Exchange Program. The paper was developed based on open source research, interviews with identified subject matter experts, and participation in industry conferences. All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts. The paper provides information concerning the current state of ransomware, the social engineering tactics used to support ransomware attacks, and an assessment of where ransomware will likely go in the next two years.

Overview

In recent years, ransomware[1] has received widespread media attention. Cyber threat actors have demonstrated an ability to successfully target individuals, companies and governments with ransomware all over the world, with victims including hospitals, police departments, universities, transportation systems, and businesses. However, ransomware is not new. Since ransomware's advent with the PC Cyborg/AIDS Trojan in 1989, the mechanism for financial gain in ransomware has been quite straightforward.[i] 2005 marked the beginning of modern ransomware, with variants using sophisticated encryption to lock files on target computers and demand payment. Today's ransomware operates on the same model, but with even more sophisticated algorithms and larger keys, making brute force decryption nearly impossible. Additionally, modern ransomware targets greater numbers of file types on the user's computer and network drives, increasing business networks' vulnerabilities. As encryption becomes more difficult to defeat, and as threat actors beyond purely financially motivated criminals continue to develop newer and greater capabilities, it is likely that intentions will go beyond simply encrypting files for the purposes of extorting money from a victim.

[1] Ransomware is a malicious software installed on a computer, network or service for the purpose of extortion. The malware encrypts the victim's data and/or systems making them unreadable. The victim will have to submit a monetary payment to a criminal(s) to decrypt files and/or regain access.

The ransomware business model is a lucrative one for cyber criminals. The average ransom amount increased from $294 in 2015 to $679 in 2016 and it is estimated that cyber criminals generated roughly $1 billion from ransomware attacks in 2016.[ii] As ransomware continues to evolve, and the proliferation of ransomware tools continues, ransom payments will likely increase and comprise a larger percentage of cybercrime costs in the near future.

In addition to paying the ransom, victims suffer additional consequences such as the loss of data, down time, reputational costs, and the expense of repairing or rebuilding their systems. According to an industry report, downtime costs North American organizations up to $700 billion annually.[iii]

The loss of data as a result of files being encrypted, can affect productivity and hinder operations. Less than half of ransomware victims are able to fully recover their data after an attack. Without access to information needed to fulfill everyday tasks, productivity and operations could be hindered and potentially result in lost sales and revenue.

As the majority of ransomware attacks are conducted for financial gain, there continues to be a shift of moving away from targeting individual or home users to targeting companies or enterprise organizations. Although there may be more barriers to successfully infecting an organization, the profit expectation (or demand) will be exponentially higher for an organization than an individual. In a 2016 study conducted by Kaspersky[iv], based on attack frequency, attacks against businesses grew by a factor of 3 while those against individuals grew by a factor of 2 from the first quarter of 2016 to the third quarter.

Three sectors that may be particularly vulnerable to ransomware are small/medium size businesses, the healthcare sector, and the education sector. The sectors, along with factors that make them vulnerable, are listed below.

- Small/Medium size businesses may lack the experience, infrastructure, and resources to maintain a strong awareness, understanding, and security posture to mitigate or remediate the threat.
- The Healthcare sector's vulnerabilities include extensive use of legacy systems, delays in patching and mitigating identified cyber threats in order to ensure safe operation of patient equipment, and widespread access to sensitive patient information, that if compromised can affect patient health and privacy.[v]
- The education sector is vulnerable due to the ease of attackers in obtaining staff information, decentralized information technology systems that increase the odds of vulnerable systems being identified, and similarities in organizational structures that allow attackers to use common attack stratagems.[vi] A recent report identified education as the most targeted sector for ransomware.[vii]

Vulnerabilities

The Internet of Things

The Internet of Things (IoT) refers to common or household devices that are "smart" or connected to the Internet. Examples include smartphones, coffee makers, wearable devices, washing machines, medical devices, and vehicles. IoT devices are already critically important in controlling power grids, water pumping stations, and medical devices.[viii] By the end of 2017, 8.4 billion connected devices will be in use and that by 2020, there will be more than 20 billion connected devices.[ix] IoT devices are an appealing target for a ransomware operation because they are interconnected and lack the security measures that desktop or laptop devices often have.[x] A private sector report claims that approximately 80% of IoT

applications and 71% of mobile applications are not tested for security vulnerabilities, thus leaving the door wide open to attackers. [xi]

Traditional ransomware has affected computers, but the increase in the number of devices connected to the Internet has provided the opportunity for systems to be controlled beyond computers.[xii] Kaspersky Labs labeled 2016 as "the year of ransomware", and the near future does not give any indication these attacks will subside.[xiii] Cyber criminals already exploit IoT vulnerabilities on a large scale. In 2016 multiple websites experienced large scale distributed denial of service attacks (DDoS) that were launched from Mirai botnets that exploited weak security on IoT devices, primarily Internet-connected cameras and digital video recorders.[xiv] On September 20, 2016, the KrebsOnSecurity website suffered one of the largest DDoS attacks ever recorded: between 600 billion and 700 billion bits per second for hours at a time, representing almost half a percent of the Internet's entire capacity.[xv] Ars Technica, hosted on a French server, also reported the same type of attack that peaked at 1.1 terabits per second, which is 60 percent larger than the Krebs site attack. [xviii]

Many medical devices, such as a pacemaker, insulin pump, or drug dispersing devices are becoming Internet-enabled.[xix] There is little security or testing of implanted medical devices.[xx] Hackers know the immediate need for these devices and could extort patients out of a great deal of money due to the patient's dependency on them. The WannaCry ransomware that affected thousands in May 2017 appears to have hit medical devices. Radiology equipment designed to help improve medical imaging has also experienced ransomware infection at a US hospital.[xxi]

Critical Infrastructure

The number of critical infrastructure sites dependent upon Internet connectivity to carry out their organization's mission continues to increase. Critical manufacturing plants, water treatment facilities, transportation, and electrical power entities are a few examples of the sectors that operate on industrial control systems (ICS) and depend upon Internet connected operations. Many ICS systems lack strong security protocols. Previous control systems were not designed for Internet connection capability, and many users make the assumption they are not on a public network and are not susceptible to an attack.[xxii]

As a demonstration of these vulnerabilities, cybersecurity researchers at the Georgia Institute of Technology (GIT) developed a new form of ransomware to take over a simulated water treatment plant.[xxiii] In the simulated attack, researchers employed ransomware to gain entry into the system and then commanded controllers to shut valves, increase the amount of chlorine added to water, and display false readings.[xxiv] The ransomware then locked infrastructure owners and operators out of the system until they

paid the ransom demand. The researchers conducted this attack simulation to highlight how the ICS that operates facilities such as manufacturing plants, water, and wastewater treatment facilities, and building management systems.[xxv] Although incidents such as this have not been reported in the real world, it is likely attackers will eventually employ attacks such as these. Similar to medical devices, these critical infrastructure sites and their operations are essential to vital services and needs for use and consumption.

Cloud Services

Cloud Services are also vulnerable to ransomware attack. The cloud has enabled more efficient data and information storage by allowing users to save to services that run on the Internet instead of a computer. This has allowed employees to work remotely, increasing productivity, allowing for better collaboration, and saving money on their information technology (IT) infrastructure.[xxvi] In RightScale's 2017 "State of the Cloud Report," 95% of organizations surveyed indicated they are running applications or experimenting with "Infrastructure-as-a-Service (IaaS).[xxvii] IaaS is one form of cloud computing where an external provider provides hardware and manages it via the Internet.[xxviii] The number of organizations that will be heavily invested in cloud computing in the future is expected to increase as many transition into full dependence on cloud technologies.[Xxix] As the number of organizations that depend on cloud technologies rises, the number of opportunities for ransomware attacks against the cloud also increases. One of the most common ways for an organization to have its cloud storage attacked is to open an infected e-mail attachment.[xxx]

Recent Developments

Ransomware-as-a-Service Business Model

Ransomware-as-a-Service (RaaS) allows cyber criminals to download a ransomware variant for free or a nominal fee. After the ransomware is deployed, if a victim pays the ransom, the original author receives a percentage of the ransom as a part of the agreement. This service is appealing to novice hackers because the most complicated part of creating ransomware is handled; a beginner only has to buy the ransomware. The service is designed so that the attacker selects their victim, enters their BitCoin wallet address, and deploys the malware.[xxxi] The service provider then takes a percentage of the ransom paid to the attacker.[xxxii]

- In May 2015, the first RaaS named "Tox" RaaS was discovered by McAfee Labs.[xxxiii] The attacker was able to determine the ransom amount and include a message with the ransomware if desired. The site generated and downloaded the virus, which was then ready to be deployed. Tox took 20% of the total ransom payout.[xxxiv] Although Tox lacked complexity and efficiency within the malicious code, it is likely that it will evolve into a large business model.[xxxv]

The techniques of RaaS provide criminals of varying backgrounds the ability to operate in the underground market and conduct effective cyber schemes for financial gain. Ransomware variants in the underground marketplace indicate the emergence of an advanced business model as capabilities provide enhanced anonymity techniques and custom solutions to criminals. Furthermore, as the ease of use in "do it yourself" ransomware packages becomes increasingly common, the business model caters to both technically savvy and less sophisticated criminals.

The following is an example of an advertisement detailing the capabilities provided by "crbr" or Cerber ransomware:

- *Complete anonymity of affiliates*
- *Real-time statistics of installs and payments on TOR affiliate panel*
- *Automated semi-monthly bitcoin payouts with options to request payout within 48 hours*
- *New binaries encrypted every 15 minutes for distribution by affiliates*
- *Ability to create sub-accounts with different ransom amount*
- *Referral system (5% additional earnings)*
- *Online support with ticketing system built into affiliate panel*
- *Actors running "Cerber" initially take 60% of the profits earned by affiliates.*
- *Cerber malware was capable of encrypting files without internet connection and did not contain any form of command and control mechanism. Additionally, cerber demonstrated professional-level coding and a mature affiliate business model.*[xxxvi]

Ransomware Attacks That Do Not Require User Interaction

The recent WannaCry and NotPetya attacks were noteworthy in their ability to spread and infect computer systems through sophisticated techniques without user interaction. Ransomware variants that exhibit these 'worm-like' qualities opens up another infection vector through the use of exploit kits, which are toolkits designed to exploit security flaws in a variety of software applications normally for the purpose of spreading malware.

WannaCry

The WannaCry attack in mid-May 2017 affected organizations worldwide leveraging a Microsoft Windows vulnerability. Microsoft had released the patches for this vulnerability two months prior to the attack - further emphasizing the importance of patch management. A key takeaway regarding the WannaCry attack was its effectiveness without relying on social engineering. Unlike traditional social engineering scenarios where user interaction is required, WannaCry utilized vulnerability (MS17-010) in Microsoft's use of Server Message Block (SMB) to automatically spread to vulnerable Microsoft Windows (Server, XP, Vista, 7, 8 and 10) networked devices using SMB.[xxxvii]

Shortly after the discovery of the WannaCry "kill switch", there was widespread media coverage attributing the attacks to amateur cyber criminals.[xxxviii] However, further research and analysis in the weeks following the initial WannaCry attack indicated possible linkages in the WannaCry malware code to that of code previously used by a North Korean State sponsored cyber group. This same North Korean group was also implicated in the 2014 attack against Sony Pictures and a multi-million dollar heist on a Bangladeshi Bank in 2016.[xxxix]

NotPetya Wiper

NotPetya hit in late June 2017, and like WannaCry utilized the same SMB vulnerability in Windows operating systems. However, it added a layer of capability to spread via other means. Researchers quickly discovered NotPetya's ability to extract credentials from an infected system, and in turn use the credentials and legitimate Windows based tools to infect other computers on the same network.[xl]

Further research showed that NotPetya was actually a destructive wiper that overwrote systems, but appeared to be ransomware.[xli] To date, this is one of the widest uses of ransomware as a smokescreen. The Ukraine based state security service, along with several security companies are initially attributing the activity to a Russian state sponsored cyber group.[xlii]

Cyber Actors and Motivations for Using Ransomware

Ransomware can be used to generate financial gain, disrupt services, deny access to information, and serve as a cover for other types of cyber attacks or exploitation. Cyber actors ranging from individuals to nation states can use ransomware to accomplish their goals. The following graphic identifies the major cyber actors, a characterization of their perceived relative technical abilities, key characteristics, and primary motivations for conducting ransomware attacks.

Social Engineering Facilitates Ransomware Attack

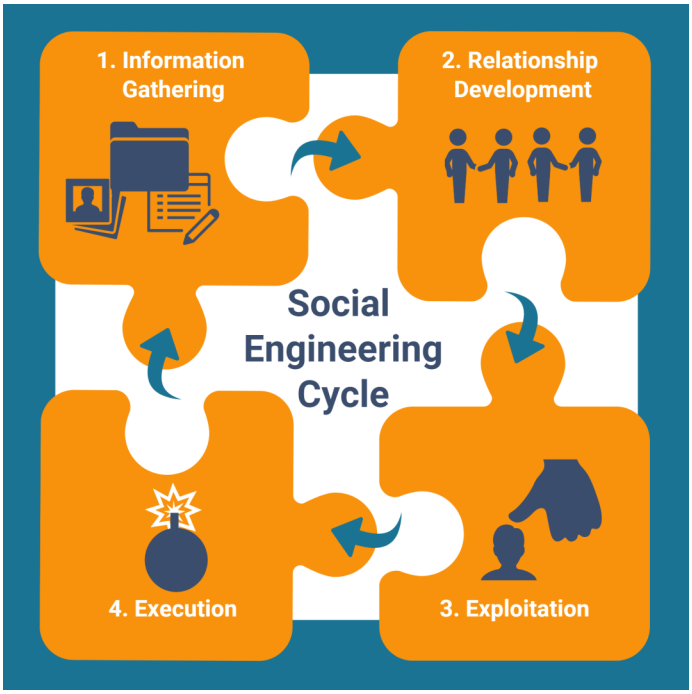
While the recent WannaCry and NotPetya attacks demonstrate how cyber criminals can deploy ransomware via exploitation of a technical vulnerability, the easiest and most common way to deploy ransomware is still sending emails with malicious attachments. The most direct way to get into a computer system is to simply ask permission. No matter how technically secure a network is, there is invariably a human factor that is susceptible to exploitation. Cyber actors use social engineering techniques to deceive, persuade, and influence targets for information that can be used to support a ransomware attack. Social engineering is defined as using human interaction to psychologically manipulate targets through deception and persuasion in order to influence the target's actions. In this section we will explore the social engineering cycle and some of the techniques cyber actors use to target potential victims.

The Cycle of Social Engineering

Social engineering typically consists of four phases: [xliii]

- Information Gathering – collecting information to help identify attack vectors and targets.
- Relationship Development – develop rapport with the target.
- Exploitation - Use information and relationships to infiltrate the target.
- Execution – Accomplish ultimate goal.

Oftentimes, however, social engineering attacks are unique, with the possibility that it might involve multiple phases and cycles, and may even incorporate the use of other more traditional attack techniques to achieve the desired end result.[xliv]



While there are in-person tactics that can be used to gather information useful in developing a strong ransomware attack, our focus is on recognizing social engineering strategies that can be employed in cyberspace or use hardware or software.

Social Engineering Tactics

Phishing

A phishing attack occurs when the attacker sends an email to someone that appears to come from a legitimate user, often asking the target to visit a compromised website or open a malicious attachment. Phishing has many variations, such as whaling, where an attacker targets executives and high-profile targets, the "big fish." If the attacker is able to glean specific information about the target, such as a name

or address, the attacker can take the phishing scam a step further and include this information in the email to make it appear even more legitimate. [xlv]

Phishing often takes advantage of information collected from social media, as users often willingly provide information via various social media sites. For example, on professional job websites, the attacker may pretend to be a job recruiter. Users post information about where they work, what they like to do, what music they like, etc. The attacker can then use this information in a number of ways:

- To impersonate a friend listed on the page by sending an email asking for confidential information;
- To view pictures of the target to determine locations they frequent and then appear at the same locations to socially engineer the target outside of a work environment;
- To discover someone's age, place of birth, school, and previous companies, which can all be used to target the person in a spear phishing attack;
- To add someone as a friend to form an online relationship with them to build trust. The social engineer then exploits that trust to get information from the target, which could be used to launch another attack;
- To send a private message to the target reference a position at a well-respected company that sounds credible; directing the target to a phishing employment site, the attacker can then gather a great deal of information, and even require the user's social security number for background check purposes. At this point, the uses for this information are practically endless.[xlvi]

Pretexting

Pretexting is presenting oneself as someone else in order to obtain private information.[xlvii] For example, a hacker may create an email address with a fake domain that looks like a targeted business executive in the "from" name. The hacker would target an individual with direct or indirect ties to their spoofed executive. Next, the attacker would monitor to see when the target will be out of the office in order to best execute their attack. For this attack, the hacker would then send a mobile text message relating to a project with the company that would be familiar to the target, calling for action by the target to review the attached files when they return to the office. Once the target returns and opens the attachments, they are infected. This technique specifically uses emotions and relationships to get employees to hastily take action.[xlvii]

Election Season

An attacker impersonates a campaign representative and calls the victim for a corporate donation. This is typically following a local election. If they pick the wrong candidate, they'll try again in a few days with the opposing candidate. The attacker will either build a website or ask for the credit card information over the phone. To finish the attack, they will often make the user fill out a form that looks like an official tax document, where they can gather more personal information about the target to reach out directly to them in the future or use their information for further gain.[xlix]

The Friendly Social Engineer

In this technique an attacker compromises a user's email or social media account, and looks at recent messages that the user has sent. Often, the initial target isn't the final target. If any links or documents have been sent, the attacker might follow up by saying they've updated the documents. For instance, if targets exchanged PDFs, the attacker could send a newly updated version with malicious code embedded. If the attacker can't find a way to breach their final target with the initial account, they may continue to look for mutual friends and try to repeat the process again.[l]

Typosquatting

Typosquatting is when the attacker sets up a website with a similar domain name to a legitimate site and waits. For example, instead of www.Legitsite.com, the attacker may register www.Legitsite.org. The spoofed site will match the look and feel of the original. The idea is to wait passively for users who mistype a URL into their web browser. They will often be prompted to enter information, which is then captured by the adversary. The victim is then forwarded over to the legitimate site oftentimes logged in but not realizing they were simply redirected and their information is now compromised.[li]

Device Left Behind

An attacker leaves a USB drive, CD-RW, phone or other storage device around an office or parking lot. In order to further entice the targets, the attacker writes a tempting label on it, such as salary information or a famous musician. This tactic takes advantage of an individual's curiosity. Also, to make sure the user thinks the device is legitimate (or to further increase their willingness to view the device), the attacker will have files that sound enticing to open, for instance "XYZ Company Salary Records.xlsx". The files have malicious software attached, thus resulting in the victim's machine being compromised.[lii]

Reverse Social Engineering

Reverse social engineering has three steps: sabotage, advertising, and assisting. In the first step, an attacker finds a way to sabotage a network. This can be as complex as launching a network attack against target's website or as simple as sending an email from a spoofed email address telling users that they are infected with a virus. No matter what technique is employed, the attacker has either sabotaged the network or given the impression that the network is sabotaged. Next, the attacker advertises their services as a security consultant. This can be done through many means including sending mailers, dropping business cards, or sending emails that advertise attacker's services. At this point, the attacker has created a problem in the network (sabotage) and is placing them in a position to help (advertising). The corporation sees the advertisement, contacts the attacker under the false pretense that the attacker is a legitimate consultant, and allows them to work on the network. Once in, the attacker gives the impression of fixing the problem (assisting) but will really do something malicious, such as planting key loggers or stealing confidential data.[liii]

Six Degrees of Separation

In this technique, an attacker reaches out to the target's friends or family, intending to develop a relationship with someone who can later "vouch" for them with the full intention of earning the trust of the target eventually. The victim will use their mutual contact to request an introduction to their target. At this point, the target is in a group setting, warmed up and comfortable, and the attacker can go after viable information. While a group might seem like a bad idea because the attacker could get caught, it could also lower someone's guard, especially if the attacker doesn't directly ask for sensitive information.

The attacker can focus on the initial victim — the mutual friend that their prime target has so much history with — and beat around the bush until they ask the question the attacker has been wanting to ask themselves.[liv]

Techie Talk

Many penetration testers and malicious hackers come from a technical background and not a background in human psychology. As a result, when technical people need to do social engineering they resort to a techie style. When an attacker calls up a user within an organization and impersonates a help desk operator the conversation on technical issues flows naturally and doesn't prompt the user to properly verify the "technician's" credentials. Simply warning users of alleged compromise of passwords and offering help to restore them sounds like routine IT assistance that can harvest valuable access information.[lv]

Cause a Panic and Take Advantage

In this situation, an attacker reaches out to a user informing they've been compromised and the attacker claims to represent a technical support individual or a help desk employee. Through data available on the Dark Net, for instance, there are numerous cases of Dell records, including service number and service call dates and information that hackers can use to not only reach out to a user but truly convince them they are technical support. Now the attacker talks to the user, saying the user needs to reset their password to meet complexity requirements, enable remote desktop access or even install a file through the command prompt. The attacker walks them through this process. After the task is completed, the attacker asks if they can help with anything else and informs the user that there is maybe a survey following this call which could be performed by the attacker's accomplice. They do this to make it seem authentic and because people tend to remember the beginning and end of conversations, but not the middle. By exiting the conversation gracefully or even adding another voice through a survey, they make it seem more authentic.[lvi]

Vishing

Vishing is an attack that uses the phone to perform the equivalent of a phishing attack. The typical target for this kind of social engineering tactic is a corporate executive. An attacker will call with a pre-recorded message, pretending to be the victim's company or the company's bank. The attacker will ask the user to call a phone number, and in doing so, they will ask for their credit card info, phone number, pin, last four digits of their social security number and other sensitive details. At this point, the attacker will report some transactions that will obviously be fake, and will cancel the transaction and promise the cardholder to send out a new card soon. The attacker will use the card for his purpose until the fraud is discovered.[lvii]

Vendor Scams for Wire Transfers

The social engineering tactic here focuses on getting money. An attacker needs to have some knowledge of the organization to pull this off on a specific target, but it can also be sent in volume acting as a big name vendor the company uses. After identifying an email marketing vendor, and using web analytics tracking software or even a content management system the attacker will be able to harvest tracking codes the company uses. The attacker will then execute a classic phishing scam, informing the victim that he is from "collections" or "accounts receivable" department. This typically happens through a phone call, but it can also come from an email as well. They'll provide an invoice for services and request payment or wire transfer to an offshore bank account. If the attacker really wants to go after someone

who initially ignores the request, he will follow up and use a voice recording from a phone call where they get the victim to answer "yes." The attacker then uses that to try to leverage payment for a product by saying that he has victim answering "yes" to being overdue for an invoice. From there, the attacker may threaten legal action.[lviii]

Future of Ransomware and Social Engineering

Over the next two years, ransomware will likely continue to be a primarily financially motivated activity, although it is likely that politically or ideologically motivated ransomware attacks will increase. As cyber actors start to employ ransomware more as a harassment tool, the breadth of targets will increase as entities may be targeted for reasons not based on assessed economic value. Financially motivated actors may broaden their mechanisms for generating profit and will likely start to combine ransomware techniques with other methods as better public awareness of the ransomware threat and increased defenses may limit the success of traditional ransomware attacks. The number of ransomware users will increase as the availability of ransomware as a service and the proliferation of ransomware exploits on the Internet suggests that technical barriers to using ransomware will decrease. Social engineering will continue to be an important tool in identifying, assessing, compromising and managing potential ransomware targets, but recent attacks have shown it is not required in all cases.

The simple approach of requiring direct cash payment from victims will likely continue to be the predominant mode of financial gain, even as the arms race continues between improved law enforcement effectiveness and the enabling impact of cryptocurrencies. However, as the problem of exfiltrating ransom payments worsens with better international law enforcement coordination, ransomware practitioners may turn to less direct, but less traceable and potentially far more effective mechanisms for realizing financial gain.

One potential area of opportunity to increase ransomware returns, as well as to compound the difficulty of tracing a given attack's origins, is market manipulation. In cases of highly publicized ransomware attacks, cybercriminals could cause share prices of a targeted company or its competitors to rise, at least temporarily. The attacker, with foreknowledge of the precipitating event, could short the targets' stocks, realizing gains limited only by initial financial resources and the need to guard against attribution. If the short-sale transactions were spread across many accounts, it would be difficult or impossible for authorities to differentiate between innocent and illicit transactions in a market with countless participants.

It is likely that ransomware users will seek to maximize potential gains by combining ransomware with other techniques such as doxware or extortionware. By first exfiltrating data from targeted computers before encrypting it, cyber actors can induce victims to not only pay to retrieve their locked computer systems, but to also prevent the public release of sensitive corporate or personal information. In cases where acquisition of intelligence is the goal, ransomware may be used to help delay or conceal knowledge of data exfiltration.[lix]

Another rising source of motivation for ransomware practitioners is likely to be hacktivism.[lx] Hacktivists can use ransomware or doxware to inflict pain on corporations and governments, to interfere with activities that the hacktivists disagree with, or to prevent or compel corporate, governmental, or individual action. As the doxware threat grows in the coming years, hacktivists may also increasingly exploit exfiltrated data to expose corporate activities to public scrutiny, which can exert pressure of

potentially market-shifting magnitude that is not otherwise available to hacktivists. Finally, hacktivists may increasingly use ransomware and doxware as a highly effective means of cyberterrorism, seeking to advance their ideological goals through shifting the behavior of targeted groups through the fear associated with cyber victimization.

Finally, as trolling and cyberbullying have become commonplace, it is likely that a genus of ransomware/ doxware practitioners will arise who do it purely "for the lulz," i.e., simply out of caprice and an enjoyment of the disturbance it causes. For example, after a zero-day exploit ransomware event, there are copycats, referred to as "script kiddies," that are racing to expose their variant creations.[lxi] Script kiddies are often juvenile hackers that use scripts written by more experienced hackers.[lxii] These kiddies copy and paste malicious code, often without an understanding of how the code works.[lxiii] Script kiddies often do not have a specific target designated for their attack, but rather scan the internet for known vulnerabilities on computer systems and select these systems to deliver their attacks. They are often referred to as "bored but curious teenagers" and do not spend a lot of time trying to break into a system with advanced defenses.[lxiv] Rather, they will focus on systems with weaknesses and vulnerabilities because it is not time-consuming. Whether the script kiddies are trying to develop something new from an original script, cause mischief, or are just curious, this could greatly impact everyday businesses and people.

There is also limited reporting indicating that cyber actors may seek to use ransomware to extract political concessions rather than money. In March 2017, ransomware named "RanRan" was detected in one Middle Eastern country.[lxv] Instead of requesting a financial payment, the ransomers attempted to extort a political statement, where the victim would create a public sub-domain appearing to encourage and incite violence against a Middle Eastern political leader.[lxvi] The ransomware also forces the victim to publically declare that they have been hacked.[lxvii]

All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.

Appendix A

Best Practices

Ransomware Defense - Best Practices

Fortunately, a majority of controls that can mitigate a ransomware attack can also be leveraged against most types of malicious activity. As such, the guidance provided in this section – while focused on ransomware – will help to mature your overall security posture if implemented properly. Below, we have provided a scenario of a *common* ransomware attack along with different controls, grouped by control type, which can aid in prevention, detection, and/or expedited response of such an attack.

Scenario

An attacker sends a spoofed email, purporting to be from a trusted vendor that is known to the organization, to your employee. The email message references an "invoice" document, which is attached to the email, and entices the recipient to open the attached Microsoft Word document. When the employee opens this malicious document, it triggers automation (macros) embedded within it that downloads and executes the ransomware on the employee's system. All non-system files have become encrypted, including those on a mapped network share used by multiple departments within your organization. The ransom note displayed to the user demands 100 Bitcoin in exchange for the key required to decrypt the files.

Email Security

Email Security Gateway

An Email Security Gateway acts as an all-in-one enterprise class solution composed of many of the email security controls discussed in this section. As emails are sent in and out of your organization, an Email Security Gateway will inspect the characteristics of each email - such as the source, destination, message contents, attachments, headers, etc. – and quarantine/drop any that were found to be suspicious.

"Cisco Email Security Appliance, Clearswift SECURE Email Gateway, Fortinet FortiMail, McAfee Security for Email Servers, Microsoft Exchange Online Protection, Proofpoint Email Protection, Sophos Email Appliance, Symantec Email Security.cloud, Symantec Messaging Gateway, Trend Micro InterScan Messaging Security, Trend Micro ScanMail Suite for IBM Domino, Trend Micro ScanMail Suite for Microsoft Exchange and Websense Email Security Gateway are some of the significant players in the email security market."[lxviii]

Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), & Domain-based Message Authentication, Reporting & Conformance (DMARC)

SPF, DKIM, and DMARC are separate-but-related controls that leverage your domain's DNS TXT record to inform the recipient of an email, that is supposedly from your organization, how to validate that said message was not forged (spoofed) and what to do should the validation fails. Specifically:

SPF tells the recipient that the email they received should have originated from one of the email servers specified within your domain's DNS TXT record.[lxix]

DKIM tells the recipient that, if the cryptographic signature of the email they received is valid, then the email was not modified in transit.[lxix]

DMARC tells the recipient what to do in the event that SPF and/or DKIM validations fail. Actions include Pass, Reject, or Quarantine of the offending email.[lxxi]

Although there is no monetary cost to utilize SPF, DKIM, or DMARC, care needs to be taken to ensure proper configuration and maintenance. Implementation of the full suite can be challenging for some organizations due to their complex environments, lack of experience, or other factors.

Real-Time Block Lists (RBL or DNSBL) / Spam Uniform Resource Identifier (URI) Real-Time Block Lists (SURBL or URI DNSBL)

RBL is a feed consisting of mail server IPs and Hostnames that have been identified as sending suspicious emails, such as spam.[lxxii]

SURBL is also a feed (or feed of feeds) that consists of website domains that have been found within the message body of suspicious/malicious emails.[lxxiii]

You should configure your email security product to routinely import both types of feeds, compare their contents to the corresponding aspects of email being inspected, and take action on the email should a match be found. For RBL, the mail servers specified within the email's headers should be inspected whereas, with SURBL, the email's message body will be compared.

Attachment Type Restriction

Restrict certain file types that would be considered risky or suspicious for your environment. The following is a comprehensive list of file types that you should consider automatically stripping from email messages at your gateway before delivery to your employees:[lxxiv]

.386	.ace	.acm	.acv	.ade	.adp	.adt	.ani	.app	.arc	.arj	.asd	.asp
.avb	.ax	.bas	.bat	.boo	.btm	.cab	.cbt	.cdr	.cer	.chm	.cla	.cmd
.cnv	.com	.cpl	.crt	.csc	.csh	.css	.dll	.drv	.dvb	.email	.exe	.fon
.fxp	.gms	.gvb	.hlp	.ht	.hta	.htlp	.htt	.inf	.ini	.ins	.iso	.isp
.its	.jar	.job	.js	.jse	.ksh	.lib	.lnk	.maf	.mam	.maq	.mar	.mat
.mau	.mav	.maw	.mch	.mda	.mde	.mdt	.mdw	.mdz	.mht	.mhtm	.mhtml	.mpd
.mpt	.msc	.msi	.mso*	.msp	.mst	.nws	.obd	.obj	.obt	.obz	.ocx	.ops
.ovl	.ovr	.pcd	.pci	.perl	.pgm	.pif	.pl	.pot	.prf	.prg	.ps1	.pub
.pwz	.qpw	.reg	.sbf	.scf	.scr	.sct	.sfx	.sh	.shb	.shs	.shtml	.shw
.smm	.svg	.sys	.td0	.tlb	.tmp	.torrent	.tsk	.tsp	.tt6	.url	.vb	.vbe
.vbs	.vbx	.vom	.vsmacro		.vss	.vst	.vsw	.vwp	.vxd	.vxe	.wbk	.wbt.
.wlz	.wk	.wml	.wms	.wpc	.wpd	.ws	.wsc	.wsf	.wsh			

**** except oledata.mso***

If an attachment is stripped, ensure to alert the user of the action so that it raises their awareness. Of course there will need to be exceptions, so if you are looking to implement this kind of control, make

sure to also implement a Secure File Sharing Portal where files such as .zip attachments can be delivered after additional scrutiny and/or validation of the sender.

Geo-Location / Domain Based Blocking

Restrict emails originating from IPs or Domains that would be considered risky or suspicious for your environment based on its associated geo-location. For example, you can dramatically reduce your organization's attack surface[lxxv] by dropping or quarantining emails originating from within a country that is under Office of Foreign Assets Control (OFAC) sanctions.[lxxvi]

Sandbox Attachments

Although a number of email security products will have the ability to scan attachments with some form of antivirus, a more comprehensive solution is to also detonate all attachments within a sandbox technology such as Cuckoo[lxxvii], Joe Sandbox[lxxviii], VxStream[lxxix], or Wildfire[lxxx] prior to delivering to the mail server. This way, behavioral characteristics of the attachment will be analyzed in additional to the static properties.

Endpoint Security

Endpoint Detection & Response (EDR)

Much like Email Security Gateways, Endpoint Detection & Response technologies act as an all-in-one solution composed of many of the endpoint security controls discussed in this section. While the cost to implement an EDR solution is significant, the consolidation of multiple platforms into one and the cross-functional (Security Operations → Incident Response → Threat Intelligence → Forensics → Etc.) utility within an organization that such a solution provides offsets the cost.

Major players in this space are RSA's NetWitness Endpoint[lxxxi], Carbon Black's Defense/Response/Protect[lxxxii], and CrowdStrike's Falcon[lxxxiii].

Antivirus

Antivirus needs no introduction. It is probably the oldest and most ubiquitous endpoint security technology out there. While Antivirus may not be as effective as one would think,[lxxiv] the concept of defense in depth[lxxxv] still applies and having Antivirus is better than not having it.

Anti-Malware

Anti-Malware is an enhanced version of Antivirus that is primarily focused on detecting cutting edge malware using the freshest indicators of compromise and heuristics. Although they perform similar functions, developers of Anti-Malware solutions suggest running Antivirus and Anti-malware in tandem.[lxxxvi]

Host-Based Intrusion Detection/Prevention System (HIDS/HIPS)

A Host-Based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. Besides such activities as dynamically inspecting network packets targeted at this specific host, a HIDS might detect which program accesses what resources and discover that, for example, a word-processor has suddenly and inexplicably started modifying the system password database. Similarly a HIDS might look at the state of a system, its stored information, whether in memory, the file system, log files or elsewhere; and check that the contents of these appear as expected, e.g. have not been changed by intruders.[lxxxvii]

In addition to detection, a Host-Based Intrusion Prevention System has the ability to actively mitigate malicious activity. For instance, you can leverage the host isolation capabilities of HIPS to lock down a system that has been compromised with ransomware in an effort to prevent further spread of the malware. Please note, however, that implementation of an Intrusion Prevention System could lead to business impact as legitimate activity could be incorrectly detected as malicious, thus triggering the prevention aspect of HIPS. It is for this reason that most organizations opt for implementing HIDS and having their security analysts perform manual verification of the alerts to confirm that response is warranted.

Ultimately, the system that you choose to implement will depend on your organization's risk appetite.

Group Policy

Windows Firewall

Malicious Downloaders[lxxxviii] and the resulting malware will typically need to reach out to a command and control (C2) server at some point in its execution. Although this is typically done via HTTP protocol, sometimes these communications take place over ports other than 80 or 443 to avoid detection. Denying all network communications occurring over non-standard ports could help to prevent a successful compromise.

Enforce Automatic Proxy Configuration

Closely related to the Windows Firewall Group Policy control, you can further restrict malicious network activity on an endpoint by explicitly forcing outbound network communications through a content filtering proxy. You then enforce the use of an automatic proxy configuration[lxxxix] to ensure your users can still access the Internet via web browsers. All other network activity should be denied.

Forcing legitimate traffic through a proxy server and implementing proper Egress filtering will prevent malware, which is not proxy-aware, from being able to contact its C2 server.

Application Mappings

Within Windows, the default file mappings for common plaint-text scripts such as Visual Basic Script (.vbs), Batch Script (.bat), JavaScript (.js), etc. are linked to the appropriate scripting engine for the file type being executed. This means that, when a user double clicks on an applicable script (eg. Script.vbs), the code within the script will execute.

As these scripts are not compiled (a.k.a plain-text), we can change the mapping of these file types via Group Policy from the default scripting engine to a text editor, like notepad.exe[xc] [xci]. This will prevent accidental execution should an unsuspecting user double-click on a malicious script that is used to download a ransomware binary.

Show File Extensions

By default, file extensions within Microsoft Windows are hidden, which makes it difficult for most users to discern the type of file that they are interacting with. Attackers often leverage this ambiguity to trick users into executing a file type that they normally wouldn't have. To remove this ambiguity, you can configure the operating system via Group Policy to display file extensions.[xc]

Disable Office Macros

Its common practice for attackers to use Office documents laced with malicious macros that are then used to download the actual ransomware. There are several triggers that can execute a macro, such as upon document opening, document closing, and image rendering.

It is highly recommended that you configure your operating systems to have Microsoft Office macros disabled and locked down by default. Individuals who have the ability to re-enable Microsoft Office macros on a case-by-case basis should be restricted to authorized personnel only.[xciii]

Execution Restriction

Application Whitelisting enables you to restrict execution to files, which you have specifically permitted to execute. This control reduces the potential for malware infection down to almost zero while also rendering other endpoint controls like Antivirus, Anti-Malware, etc. as insignificant. Unfortunately, while this is the preferred control, the resources required to configure and maintain such as control makes it a non-starter for most large, complex, and/or unstructured environments.

Application Blacklisting is the process of restricting the execution of files that are known to be bad. Since the maintenance required to successfully implement Application Whitelisting is unrealistic for most organizations, Application Blacklisting is a nice alternative that compliments other endpoint security controls such as Antivirus.

Lastly, preventing the execution of files that are located within certain directories should be considered as well as malware authors will typically hide their malware within folders that the user has write

permissions to, such as:[xciv]

- C:\Temp\
- %LocalAppData%
- %AppData%

While you can use Group Policy to perform basic execution restriction,[xcv] more advanced capabilities - such as blocking/allowing execution based on a file's hash value - can be enabled via Windows AppLocker.[xcvi]

Network Security

Content Filtering Proxy

Malicious C2 domains/servers are often "uncategorized", newly created, or are categorized as "malicious". Organizations should implement a content filtering proxy and configure it to block sites that are either brand new or have categorizations that have been deemed as risky/suspicious/ malicious for their environment.

In the event that you cannot outright block a categorization because of business reasons, your organization should implement a "click-thru" splash page that is presented to the user, notifying them of the potential danger of the page they are trying to visit. This requires that the user manually interact with the splash page if they wish to proceed to the website in question; a concept similar to CAPTCHA[xcvii].

If a ransomware executable is proxy aware and the categorization for the C2 domain that it is attempting to access is permitted, it likely won't know how to navigate past this click-thru page; thus, network communication with the C2 server will fail.

Egress Filtering

Much like the Windows Firewall control discussed in the Group Policy section, there is a similar control at the network level. It is suggested that you force any internal-to-external network traffic through a Forward Proxy.[xcviii] Then, configure your perimeter firewalls to only permit outbound network traffic if it is originating from said proxy. Preventing your endpoints from directly accessing the Internet will dramatically reduce the likelihood of successful C2 communications for malware that is either not proxy aware or that uses non-standard ports.

Network-Based Intrusion Detection/Prevention System (NIDS/NIPS)

When malware is created, the developer explicitly permits the malware user the ability to define a minimum variables required to customize the malware for their application. Typically, these are values such as C2 IP addresses, C2 domains, and bitcoin wallet addresses. The underlying code and network communication structure, however, will remain static and therefor predictable and detectable.

A Network-Based Intrusion Detection System (NIDS) will monitor all inbound/outbound network traffic and, should any traffic match the pattern specified within your rule set, take whatever action you have defined. This can include simply logging the event, alerting your security team, or - in the case of a

Network-Based Intrusion Prevention System (NIPS) - dropping the traffic.

Popular NIDS/NIPS solutions include Snort[xcix], Suricata[c], and Bro[ci]. EmergingThreats[cii] also provides a robust set of signatures[ciii], both free and paid, for Snort and Suricata that can get you up and running quickly. As these technologies are Open Source, it is easy for you to develop your own content and/or functionality as needed.

Access & Identity Management

Least Privilege / Privilege Separation

Users require different levels of permissions to perform different functions while at work. It is good security practice to require a different set of credentials based on the privilege level required to perform the task.

For example, you would want to restrict privileges on the account that will be used to interact with sources containing potentially malicious content such as email and the Internet. This type of account should be considered high risk and, as such, should not have the ability to install software, modify system configurations, administer other systems, or any other type of administrative function.

If the user requires this ability, they should be provisioned a separate 'administrative account' that they can use to perform these administrative functions. As this is a privileged account, it is imperative that it not have the ability to access email, the Internet, etc.

Specifically, the instance where ransomware has caused the most damage is when a user's access rights to a network share have not been applied in a least privilege configuration. A compromised user asset with full access to an organization's file share can result in all files within the entire share becoming encrypted.

Incident Response

Security Team Notification Mechanisms

Your Cyber Incident Response Team (CIRT) should have multiple methods defined for how users can engage them in the event they identify a suspicious file, system activity, etc. Examples of notification methods include:

- Email Distribution List / Mailbox
- Ticket Queue
- Telephone Hotline

These contact methods should be routinely socialized throughout your organization so that, if/when a malware outbreak occurs, your users are able to quickly notify your CIRT, which will result in expedited containment of the threat.

Well-defined Incident Response (IR) Plan

Implement a well-defined and often studied Incident Response plan. This will be the CIRT's guiding light

in the fog of cyber war. If/when you get hit with ransomware, having a strategy in place that is second nature to your security analysts will save valuable amounts of time, effort, and -in the case of ransomware- data. Two different Incident Response methodologies that you can use as the foundation for your Incident Response plan are SANS PICERL[civ] and NIST's SP.800-61[cv].

Threat Containment

In the event of a ransomware outbreak, your CIRT will require the ability to quickly isolate the infected system(s) from the rest of the organization to prevent further impact. Just as you should have multiple overlapping controls to protect yourself in the event that one fails, your CIRT should also have multiple methods for containing a threat. What follows are a few suggested processes/capabilities that you should considering implementing:

- Host-Based isolation via Windows Firewall
- Host-Based Isolation via HIPS
- Virtual Machine isolation / Virtual Isolation
- Network-based switch port isolation
- Network-based site isolation (building/state/country)
- Wireless network-based host isolation
- Physical network disconnect
- VPN isolation
- User account isolation (disable/restriction)
- IP/Domain block via proxy/firewall

When implementing these controls, it is important that you configure them to still allow for inspection of the isolated host by your CIRT and their toolset. For example, your CIRT should be on their own dedicated Virtual Local Area Network (VLAN) and said VLAN should be allowed, within the isolation control configuration, to establish connections to the isolated host.

Email Purge

This is associated with Threat Containment but is importation enough to give it its own section. Email is a major vector for delivering malware and with user click-rates reaching ~24% when it comes to malicious email, attackers are finding success in numbers. As such, it is important that your CIRT has a process for quickly purging emails identified as malicious from your mail server and your user's inboxes to limit exposure.

Education & Training

Security Awareness

Organizations should implement a formalized Security Awareness Program where employees are routinely educated and tested on:

1. Common Social Engineering tactics that malicious actors will use to "exploit the human."
2. How to identify and report suspicious emails, files, and activity.
3. How to report something that is suspicious.

The primary goal of this program should be to engrain security best practice into corporate culture.

Security Analyst Skills Training

One of the more critical components to any security program is having a capable team of analysts that are responsible for identifying and responding to malicious activity. In order to be successful, you must ensure that these analysts are routinely trained on common tactics, techniques, and procedures (TTP)[cvii] employed by malicious actors.

The default solution is to provide your employees with access to industry-recognized trainings/ certifications such as CompTia's Network+[cviii] and Security+[cix] for your entry-level analysts, and GIAC's Certified Incident Handler (GCIH)[cx] and Certified Intrusion Analyst (GCIA)[cxi] for your intermediary analysts.

Additionally, it is recommended that you develop an internal training program that will not only help to prepare the analyst for the external certifications but will also provide them with education targeted to your organization such as organizational structure, enterprise security toolsets, etc.

Business Restoration

Don't pay the ransom: Restore from backups

This is probably the most important control in this list. The reality is that, even if you implement every single one of these controls, you still run the risk of becoming infected with ransomware. The only way for you to truly minimize the potential impact that a ransomware outbreak could have on your organization is to ensure that you have a robust data backup strategy in place.

One such strategy is referred to as the "3-2-1 rule"[cxii]. This involves having at least 3 total copies of your data: 2 of which are local but on different mediums (ex. Network Attached Storage, On-Site Tapes, External Hard Drives, etc.) and at least 1 copy offsite.

With such a strategy in place, restoring your business after a major ransomware attack is trivial.

Don't pay the ransom: Decryption Services

A large number or ransomware variants chose to encrypt files using a custom self-developed algorithm rather than tried-and-true standard asymmetric encryption. When this happens, security researchers are able to reverse engineer the custom algorithm and develop their own decryptors.

Once such resource is a website called No More Ransom (nomoreransom.org), which is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, and two cyber security companies – Kaspersky Lab and McAfee – with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.[cxii]

No More Ransom contains decryptors for over 85 different variants of ransomware.

Pay the ransom: Stockpile Bitcoin

A growing trend amongst organizations is the stockpiling of Bitcoin in preparation for a ransomware attack. The thought being that, if hit with ransomware, the organization would be able to quickly pay the ransom, which would result in the expedited decryption of files and restoration of business.

While the U.S. Government does not recommend paying the ransomware,[cxiv] ultimately it is a business decision that needs to be made by executive leadership and/or the board of directors well in advance of an attack.

Reduce Impact: Cyber Insurance

New kid on the block is Cyber Insurance. As the concept is still in its infancy, it is hard to tell the level of coverage that Cyber Insurance could provide in the event of a major ransomware event. Cyber insurance goes beyond general liability or business operator policies to cover the expense of hiring experts to defend you and get you up and running again. It can also cover lost income due to service outages, third party and privacy liability, as well as provide reimbursement for ransomware payments. While Cyber Insurance won't help you get your data back, it can help hedge any financial losses that result from a business outage.

References

[i] DeLoitte Threat Intelligence and Analytics. (2016, August 12). *Ransomware: Holding Your Data Hostage.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf

[ii] (2017). *Internet Security Threat Report.* Retrieved from Symantec: https://www.symantec.com/security-center/threat-report

[iii](2017). *What is Ransomware and What is its Financial Impact?* Retrieved from http://www.dynamixsolutions.com/what-is-ransomware-and-what-is-its-financial-impact/

[iv]Anton Ivanov, D. E. (2016, December 8). *Kaspersky Security Bulletin 2016. The ransomware revolution*. Retrieved from SecureList.com: https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/

[v] BitSight Technologies(2017). *The Rising Face of Cyber Crime: Ransomware.* Retrieved from https://cdn2.hubspot.net/hubfs/277648/Insights/BitSight_Insights_-_The_Rising_Face_of_Cyber_Crime_Ransomware.pdf?t=1498240749814&utm_source=hs_automation&utm_medium=email&utm_content=34582971&_hsenc=p2ANqtz-_0W-DF2DBCAsiCOBab_s2GRb52c29yWSGL2g5o883V8mW9_UmZEGQl_aMLLEQCec_W0lSD7DGBNU8ems-_ImxGa8fNHQ&_hsmi=34582971

[vi] Jarosch, A. (2017, January 23). *Why Higher Education is Now the Top Ransomware Target*. Retrieved from code42.com: http://blog.code42.com/why-higher-education-is-now-the-top-ransomware-target/

[vii] Dickson, Ben. (2016, October 2). *What makes IoT ransomware a different and more dangerous threat?* Retrieved from TechCrunch. https://techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-dangerous-threat/, Accessed on 06/05/2017.

[viii] Dickson, Ben. (2016, October 2). *What makes IoT ransomware a different and more dangerous threat?* Retrieved from https://techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-dangerous-threat/ Accessed on 06/05/2017.

[ix] Van Der Meulen, Rob (2017, February 7) *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Retrieved from http://www.gartner.com/newsroom/id/3598917, Accessed on 06/21/2017.

[x] Cluley, Graham. (2016, April 27). *Ransomware and the Internet of Things.* Welivesecurity. https://www.welivesecurity.com/2016/04/27/ransomware-internet-things/, Accessed on 06/05/2017.

[xi] Forrest, Conner. (2017, January 18). *80% of IoT apps not tested for vulnerabilities, report says.* TechRepublic. http://www.techrepublic.com/article/80-of-iot-apps-not-tested-for-vulnerabilities-report-says/, Accessed on 06/15/2017.

[xii] Theim, Courtney. (2016, December 27). *2017 Predictions: Ransomware of Things Will Rise*. SecureWorld. https://www.secureworldexpo.com/industry-news/2017-predictions-ransomware-of-things-will-rise, Accessed on 06/05/2017.

[xiii] Kaspersky (2016) *Kaspersky Security Bulletin 2016*. Retrieved from https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf, Accessed on 06/14/2017.

[xiv] Symantec (2016, October 26) *Mirai: what you need to know about the botnet behind recent major DDoS attacks.* Retrieved from: https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

[xv] Blumenthal, Eli and Weise, Elizabeth. (2016, October 21). *Hacked home devices caused massive Internet outage.* Retrieved from: https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/, Accessed on 06/05/2017.

[xvi] The Economist. (2016, October 8). *The internet of stings.* Retrieved from: http://www.economist.com/news/science-and-technology/21708220-electronic-tsunami-crashes-down-solitary-journalist-internet, Accessed on 05/02.2017.

[xvii] Ibid

[xviii] Gooden, Dan (2016, September 28) *Record-breaking DDoS reportedly delivered by >145k hacked cameras.* Retrieved from https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/
[xix] McAfee Labs (2016, November). *McAfee Labs 2017 Threat Predictions*. Retrieved from: https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf, Accessed on 06/14/2017.
[xx] IT-Online (2017, March 21). *Could cyber-hackers break your heart?* Retrieved from: https://it-online.co.za/2017/03/21/could-cyber-hackers-break-your-heart/, Accessed on 06/15/2017.
[xxi] Fox-Brewster, Thomas. (2017, May 17). *Medical Devices Hit By Ransomware For The First Time in US Hospitals.* Retrieved from: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4e2edbc6425c, Accessed on 06/15/2017.
[xxii] Toon, John. (2017, February 13). *Simulated Ransomware Attack Shoes Vulnerability of Industrial Controls.* Georgia Institute of Technology. Retrieved from: http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls, Accessed on 06/22/2017.
[xxiii] Toon, John (2017, February 13) *Simulated Ransomware Attack Shows Vulnerability of Industrial Controls.* Retrieved from http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls
[xxiv] Ibid
[xxv] Ibid
[xxvi] Budd, Christopher. (2016, July 20). *Ransomware infects the cloud: What you need to know*. Retrieved from http://blog.trendmicro.com/ransomware-infects-the-cloud-what-you-need-to-know/
[xxvii] Columbus, Louis. (2017, February 18). *RightScale 2017 State Of The Cloud Report: Azure Gaining in Enterprises*. Forbes. Retrieved on: https://www.forbes.com/sites/louiscolumbus/2017/02/18/rightscale-2017-state-of-the-cloud-report-azure-gaining-in-enterprises/#1171bdff8481, Accessed on 06/20/2017.
[xxviii] Interoute Communications Limited (2017) *What is Iaas?* Retrieved from: http://www.interoute.com/what-iaas, Accessed on 06/20/2017.
[xxix] Newtek- Your Business Solutions Company. (2015, July 5). *The Future of the Cloud.* Forbes. https://www.forbes.com/sites/thesba/2015/07/08/the-future-of-the-cloud/#469358c34223, Accessed on 06/20/2017.
[xxx] Budd, Christopher. (2016, July 20). *Ransomware infects the cloud: What you need to know.* Trend Micro Incorporated. Retrieved on: http://blog.trendmicro.com/ransomware-infects-the-cloud-what-you-need-to-know/, Accessed on 06/20/2017.
[xxxi] Bailey, Katelyn. (2017). *2016: The Year of Ransomware.* The Center for Internet Security. Retrieved from: https://www.cisecurity.org/2016-the-year-of-ransomware/, Accessed on 06/06/2017.
[xxxii] Ibid
[xxxiii] McAfee Labs. (2015, May 23). *Meet 'Tox': Ransomware for the Rest of Us*. Retrieved from: https://securingtomorrow.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/, Accessed on 06/07/2017.
[xxxiv] Ibid
[xxxv] Ibid
[xxxvi] Trendmicro (2017 September 02). *Ransomware as a Service: ransomware operators find ways to bring in business* Retrieved from: https://www.trendmicro.com/vinfo/us/security/news/cybercrim-and-digitial-threats/ransomware-operators-find-ways-to-bring-in-business Accessed on 07 March 2017
[xxxvii] Woollaston, V. (2017, May 22). *WannaCry ransomware: what is it and how to protect yourself*. Retrieved from wired.co.uk: http://www.wired.co.uk/article/wannacry-ransomware-virus-patch
[xxxviii] Kaste, M. (2017, May 16). *From Kill Switch to Bitcoin, 'WannaCry' Showing Signs of Amateur Flaws*. Retrieved from npr.org: http://www.npr.org/sections/alltechconsidered/2017/05/16/528570788/from-kill-switch-to-bitcoin-wannacry-showing-signs-of-amateur-flaws
[xxxix] Solon, O. (2017, May 15). *WannaCry ransomware has links to North Korea, cybersecurity experts say*. Retrieved from theguardian.com: https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group

[xl] Bisson, D. (2017, June 28). *NotPetya: Timeline of a Ransomworm*. Retrieved from tripwire.com: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/
[xli] Duckett, C. (2017, June 29). *Ransomware in disguise: Experts say Petya out to destroy not ransom*. Retrieved from zdnet.com: http://www.zdnet.com/article/ransomware-in-disguise-experts-say-petya-out-to-destroy-not-ransom/
[xlii] Fox-Brewster, T. (2017, July 3). *NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid'*. Retrieved from Forbes.com: https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/
[xliii] Nyirak, A. (n.d.). *The Social Engineering Framework.* Retrieved August 09, 2017, from https://www.social-engineer.org/framework/attack-vectors/attack-cycle/
[xliv] Allen, M. (2006, June). *Social Engineering: A Means To Violate A Computer System*. Retrieved August 09, 2017, from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529
[xlv] Whitaker, A. (2009, June 11). *Top 10 Social Engineering Tactics: Catch Me a Phish.* Retrieved from https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat-business
[xlvi] Whitaker, A. (2013, June 11). *Top 10 Social Engineering Tactics*. *Social (Engineer) Networking*. Retrieved August 09, 2017, from http://www.informit.com/articles/article.aspx?p=1350956&seqNum=7
[xlvii] 2017 Social Engineer, Inc. *The Social Engineering Framework: Pretexting.* Retrieved August 09, 2017, from https://www.social-engineer.org/framework/influencing-others/pretexting/
[xlviii] 2017 Social Engineer, Inc. *The Social Engineering Framework: Successful Pretexting*. Retrieved August 09, 2017, from https://www.social-engineer.org/framework/influencing-others/pretexting/
[xlix] Peterson, C. (2016, March 16). *23 Social Engineering Attacks You Need To Shut Down: Election Season*. Retrieved August 09, 2017, from https://www.smartfile.com/blog/social-engineering-attacks/
[l] Zorz, M. (2016, May 19). *The life of a social engineer: Hacking the human*. Retrieved August 09, 2017, from https://www.helpnetsecurity.com/2016/05/19/social-engineer/
[li] Peterson, C. (2016, March 16). *23 Social Engineering Attacks You Need To Shut Down: Typosquatting.* Retrieved August 09, 2017, from https://www.smartfile.com/blog/social-engineering-attacks/
[lii] Peterson, C. (2016, March 16). *23 Social Engineering Attacks You Need To Shut Down: Device Left Behind.* Retrieved August 09, 2017, from https://www.smartfile.com/blog/social-engineering-attacks/
[liii] Whitaker, A. (2009, June 11). *Top 10 Social Engineering Tactics: Techie Talk.* Retrieved August 09, 2017, from https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat-business
[liv] Peterson, C. (2016, March 16). *23 Social Engineering Attacks You Need To Shut Down: Six Degrees of Separation*. Retrieved August 09, 2017, from https://www.smartfile.com/blog/social-engineering-attacks/
[lv] Whitaker, A. (2009, June 11). *Top 10 Social Engineering Tactics: Techie Talk*. Retrieved August 09, 2017, from https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat-business
[lvi] CSO Magazine. (2012) *The Ultimate Guide to Social Engineering*. Retrieved August 09, 2017, from http://core0.staticworld.net/downloads/idge/imported/article/cso/2012/02/social-engineering-ultimate-guide.pdf
[lvii] Whitaker, A. (2009, June 11). *Top 10 Social Engineering Tactics: Catch Me a Vish*. Retrieved August 09, 2017, from https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat-business
[lviii] Mogil Organization. (2016, March 23). *Risk Bulletin: Social Engineering Wire Transfer Scams Affecting U.S. Companies.* Retrieved August 09, 2017, from http://mogil.com/risk-bulletin-social-engineering-wire-transfer-scams-affecting-u-s-companies/
[lix] Countercept. (2017, March 25). *Cyber Attacks – What Are the Financial Impacts?* Retrieved from: https://www.countercept.com/our-thinking/how-much-should-you-care-about-cybersecurity/
[lx] Wagstaff, Keith. (2016, January 2). *Hack to the Future: Experts Make 2016 Cybersecurity Predictions.* Retrieved from: http://www.nbcnews.com/tech/internet/hack-future-experts-make-2016-cybersecurity-predictions-n486766
[lxi] PC Tools by Symantec (2017) *What is a Script Kiddie?* Retreived from: http://www.pctools.com/security-news/script-kiddie/, Accessed on 06/07/2017.

[lxii] Ibid
[lxiii] Ibid
[lxiv] Carson, Joseph and Singh, Amar. (2017, April 6). *Debunking the 5 Myths of Sophisticated Cyber Attacks*. Security Magazine. Retrieved from: http://www.securitymagazine.com/articles/87953-debunking-the-5-myths-of-sophisticated-cyber-attacks, Accessed on 06/07/2017.
[lxv] Cimpanu, Catalin. (2017, March 9). New RanRan Ransomware Uses Encryption Tiers, Political Messages. BleepingComputer. https://www.bleepingcomputer.com/news/security/new-ranran-ransomware-uses-encryption-tiers-political-messages/, Accessed on 06/06/2017.
[lxvi] Ibid
[lxvii] Ibid
[lxviii] Scarfone, K. (n.d.). *Comparing the best email security gateways*. Retrieved August 03, 2017, from: http://searchsecurity.techtarget.com/feature/Comparing-the-best-email-security-gateways
[lxix] Mehnle, J. (Ed.). (2010). *Sender Policy Framework*. Retrieved August 03, 2017, from http://www.openspf.org/Introduction
[lxx] Crocker, D. (2007, October 16). *DKIM Frequently Asked Questions*. Retrieved August 03, 2017, from http://dkim.org/info/dkim-faq.html#basics
[lxxi] DMARC Overview. (n.d.). Retrieved August 03, 2017, from https://dmarc.org/overview
[lxxii] DNSBL. (2017, July 28). Retrieved August 03, 2017, from https://en.wikipedia.org/wiki/DNSBL
[lxxiii] SURBL. (2017, July 20). Retrieved August 03, 2017, from https://en.wikipedia.org/wiki/SURBL
[lxxiv] @nyxbone. (n.d.). *Ransomware Overview*. Retrieved August 07, 2017, from https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml
[lxxv] Newman, L. H. (2017, June 03). *Hacker Lexicon: What Is an Attack Surface?* Retrieved August 07, 2017, from https://www.wired.com/2017/03/hacker-lexicon-attack-surface/
[lxxvi] U.S. Treasury. (n.d.). *Office of Foreign Assets Control - Sanctions Programs and Information*. Retrieved August 07, 2017, from https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx
[lxxvii] Cuckoo (n.d.) Malware? Tear it apart, discover its ins and outs and collect actionable threat data. Cuckoo is the leading open source automated malware analysis system. Retrieved August 07, 2017, from https://cuckoosandbox.org/
[lxxviii] LLC, J. S. (n.d.). *Analyse Malware in a Depth Previously Not Possible*. Retrieved August 07, 2017, from https://www.joesecurity.org/
[lxxix] Payload Security (n.d.) *Automated Malware Analysis - VxStream Sandbox.* Retrieved August 07, 2017, from https://www.payload-security.com/products/vxstream-sandbox
[lxxx] PaloAlto Networks (n.d.) *WildFire.* Retrieved August 07, 2017, from https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/wildfire
[lxxxi] RSA (n.d.) *Endpoint Threat Detection & Response.* Retrieved August 07, 2017, from https://www.rsa.com/en-us/products/threat-detection-and-response/endpoint-threat-detection-and-response
[lxxxii] Carbon Black Inc. (n.d.). *Endpoint Security Products & Next-Gen Antivirus* | Retrieved August 07, 2017, from https://www.carbonblack.com/
[lxxxiii] CrowdStrike (n.d.) Crowdstrike Falcon. Retrieved August 07, 2017, from https://www.crowdstrike.com/products/
[Lxxxiv] Vigna, G. (2014, May 21). *Antivirus Isn't Dead, It Just Can't Keep Up*. Retrieved August 07, 2017, from https://www.lastline.com/labsblog/antivirus-isnt-dead-it-just-cant-keep-up/
[lxxxv] Security Magazine (n.d.) *Defense in Depth: A Layered Approach to Network Security.* Retrieved August 07, 2017, from http://www.securitymagazine.com/articles/85788-defense-in-depth-a-layered-approach-to-network-security
[lxxxvi] Zamora, W. (2016, March 28). *What's the difference between antivirus and anti-malware?* Retrieved August 07, 2017, from https://blog.malwarebytes.com/101/2015/09/whats-the-difference-between-antivirus-and-anti-malware/
[lxxxvii] Wikipedia.org (2017, July 30) *Host-based intrusion detection system.* Retrieved August 07, 2017, from https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

[lxxxviii] Symantec (n.d.) *Downloader.* Retrieved August 07, 2017, from https://www.symantec.com/security_response/writeup.jsp?docid=2002-101518-4323-99
[lxxxix] Wikipedia.org (2017, July 12) *Proxy auto-config.* Retrieved August 07, 2017, from https://en.wikipedia.org/wiki/Proxy_auto-config
[xc] Bluesoul.me (2016, May 12) *Use GPO to change the default behavior of potentially malicious file extensions.* (2016, May 12). Retrieved August 07, 2017, from https://bluesoul.me/2016/05/12/use-gpo-to-change-the-default-behavior-of-potentially-malicious-file-extensions/
[xci] Microsoft.com (n.d.) *Configure an Open With Item.* Retrieved August 07, 2017, from https://technet.microsoft.com/en-us/library/cc732272(v=ws.11).aspx
[xcii] Microsoft.com (n.d.). *Folder Options Extension.* Retrieved August 07, 2017, from https://technet.microsoft.com/en-us/library/cc731818(v=ws.11).aspx
[xciii] Balan, D. (n.d.). *Microsoft Project – how to control Macro Settings using registry keys*. Retrieved August 07, 2017, from https://blogs.technet.microsoft.com/diana_tudor/2014/12/02/microsoft-project-how-to-control-macro-settings-using-registry-keys/
[xciv] @nyxbone. (n.d.). *Ransomware Overview.* Retrieved August 07, 2017, from https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml
[xcv] Bartlett, M. (2015, December 12). *Prevent Users From Running Certain Programs.* Retrieved August 07, 2017, from https://www.technipages.com/prevent-users-from-running-certain-programs
[xcvi] DFIR-blog.com (2016, January 03). *Protecting Windows Networks – AppLocker.* Retrieved August 07, 2017, from https://dfir-blog.com/2016/01/03/protecting-windows-networks-applocker/
[xcvii] Wikipedia.org (2017, August 07). *CAPTCHA.* Retrieved August 07, 2017, from https://en.wikipedia.org/wiki/CAPTCHA
[xcviii] Ellrod, C. (2010, October 04). *Reverse vs. Forward Proxy.* Retrieved August 07, 2017, from https://www.citrix.com/blogs/2010/10/04/reverse-vs-forward-proxy/
[xcix] Snort.org (n.d.). *Snort - Network Intrusion Detection & Prevention System.* Retrieved August 07, 2017, from https://www.snort.org/
[c] Suricata. (n.d.). *Suricata* Retrieved August 07, 2017, from https://suricata-ids.org/
[ci] Bro.org (n.d.). *The Bro Network Security Monitor.* Retrieved August 07, 2017, from https://www.bro.org/
[cii] Emergingthreats.net (n.d.). *About Emerging Threats.* Retrieved August 07, 2017, from http://doc.emergingthreats.net/bin/view/Main/AboutEmergingThreats
[ciii] Emergingthreats.net (n.d.). *Emerging Threats.net Open rulesets.* Retrieved August 07, 2017, from https://rules.emergingthreats.net/
[civ] Kral, P. (2011, December 5). *The Incident Handlers Handbook.* Retrieved August 7, 2017, from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
[cv] National Institute of Standards & Technology. (2012, August). *Computer Security Incident Handling Guide.* Retrieved August 7, 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[cvi] Phishme.com (n.d.). *2016 Enterprise Phishing Susceptibility Report.* Retrieved August 07, 2017, from https://phishme.com/2016-enterprise-phishing-susceptibility-report/
[cvii] Optiv.com (n.d.). *Tactics, Techniques and Procedures (TTPs) Within Cyber Threat Intelligence.* Retrieved August 07, 2017, from https://www.optiv.com/blog/tactics-techniques-and-procedures-ttps-within-cyber-threat-intelligence
[cviii] Comptia.org (n.d.). *CompTIA Network.* Retrieved August 07, 2017, from https://certification.comptia.org/certifications/network
[cix] Comptia.org (n.d.). *CompTIA Security.* Retrieved August 07, 2017, from https://certification.comptia.org/certifications/security
[cx] Giac.org (n.d.). *Security Certification:* GCIH. Retrieved August 07, 2017, from https://www.giac.org/certification/certified-incident-handler-gcih

[cxi] Giac.org (n.d.). *Security Certification: GCIA.* Retrieved August 07, 2017, from https://www.giac.org/certification/certified-intrusion-analyst-gcia
[cxii] Taggart, J. (2017, May 30). *3, 2, 1, GO! Make backups of your data!* Retrieved August 07, 2017, from https://blog.malwarebytes.com/101/2017/04/3-2-1-go-make-backups-of-your-data/
[cxiii] Nomoreransom.org (n.d.). *No More Ransom!: About the Project.* Retrieved August 07, 2017, from https://www.nomoreransom.org/en/about-the-project.html
[cxiv] Federal Bureau of Investigation. (2016, July 14). *Ransomware Prevention and Response for CISOs.* Retrieved August 07, 2017, from https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view